UNITED STATES OF AMERICA	)	
	)	
v.	)	**Government Targeted Brief**
	)	**on Admissibility of**
Manning, Bradley E.	)	**Internet Documents**
PFC, U.S. Army,	)	
HHC, U.S. Army Garrison,	)	
Joint Base Myer-Henderson Hall	)	**15 June 2013**
Fort Myer, Virginia 22211	)	

FACTS

The accused is charged with giving intelligence to the enemy, in violation of Article 104, Uniform Code of Military Justice (hereinafter "Article 104" and "UCMJ," respectively). The accused is also charged with causing intelligence to be "wrongfully and wantonly" published in violation of Article 134, UCMJ, eight specifications alleging misconduct in violation of 18 U.S.C. § 793(e), five specifications alleging misconduct in violation of 18 U.S.C. § 641, two specifications alleging misconduct in violation of 18 U.S.C. § 1030(a)(1), and five specifications alleging misconduct in violation of Article 92 of the UCMJ. *See* Charge Sheet.

The accused pleaded guilty by exceptions and substitutions to Specifications 2, 3, 5, 7, 9, 10, 13, 14 and 15 of Charge II. See Appellate Exhibit CDLXIV. The accused did not plead guilty *inter alia*, to Specifications 4, 6, 8, 11, 12, and 16 of Charge II. See *id.*

On 10 June 2013, the Court asked the parties to brief the following issues: (1) the requirements to authenticate tweets and the Internet Archive result, (2) the admissibility of the tweets and Internet Archive result with respect to hearsay, and (3) the relevance of the tweets and Internet Archive result.

BURDEN OF PERSUASION AND BURDEN OF PROOF

At trial, the United States "bears the burden of establishing an adequate foundation for admission of evidence against an accused." *United States v. Lubich*, 72 M.J. 170, 173 (C.A.A.F. 2013) (citing *United States v. Maxwell*, 38 M.J. 148, 150 (C.M.A. 1993). The United States may meet its burden of proof with direct or circumstantial evidence. *Id.* (citing *United States v. Freeman*, 65 M.J. 451, 453 (C.A.A.F. 2008).

WITNESSES/EVIDENCE

The United States respectfully requests that the Court consider the Enclosures referenced herein. The United States submits Enclosure 1, Enclosure 2, and Enclosure 3 to support authentication. *See* Military Rule of Evidence (hereinafter "MRE") 104(a). The United States does not presently intend to submit Enclosure 1, Enclosure 2, nor Enclosure 3 as evidence for the trial. The United States will move to introduce Enclosure 4 as evidence.

APPELLATE EXHIBIT 567
PAGE REFERENCED: ____
PAGE ____ OF ____ PAGES

LEGAL AUTHORITY AND ARGUMENT

I. AUTHENTICATION

Authentication is governed by the lax standards set out in MRE 104(b) and 901(a). David A. Schlueter, et al., *Military Evidentiary Foundations* § 4-10[2] 131 (4th ed. 2010). A proper foundation guarantees that the fact finder could find that particular evidence is what it purports to be. *United States v. Schmable* 58 M.J. 643, 653 (N-M. Ct. Crim. App. 2003). Authentication requires a preliminary determination whether sufficient proof exists for a reasonable fact finder to determine authenticity. *Lubich*, 72 M.J. at 174 (citing *United States v. Sliker*, 751 F.2d 477 (2d Cir. 1984)). For digital data, the fact that it is possible to alter the data only goes to the weight of the evidence and not its admissibility. *United States v. Hock Chee Koo*, 770 F.Supp.2d 1115, 1122-23 (D. Or. 2011) (citing *United States v. Bonallo*, 858 F.2d 1427, 1436 (9th Cir. 1988); *United States v. Safavian*, 435 F.Supp.2d 36, 39-40 (D.D.C. 2006). The fact that digital data may be altered does not preclude authentication. *Id.*

In the instant matter, the United States sets forth the basis of the admissibility of the three Prosecution Exhibits (hereinafter "PE") for Identification listed herein. The United States offers PE 31 for Identification (hereinafter "email tweet") as a tweet from the WikiLeaks Twitter account on 7 May 2010.[1] The United States offers PE 32 for ID as another tweet from the WikiLeaks account (hereinafter "video tweet") on 8 January 2010. The United States offers PE 109 for ID as a portion of the WikiLeaks website as captured by the Internet Archive (hereinafter "Most Wanted List") on 5 November 2009 at 06:13:30.

A. Tweets Authentic Based on Internal Characteristics

MRE 901(b)(4) permits authentication based on the evidence's "appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with the circumstances." In particular, the content of the information can authenticate the tweet. *See Lubich*, 72 M.J. at 175. Both the email tweet (PE 31 for Identification) and video tweet (PE 32 for Identification) display distinct characteristics attributable to WikiLeaks. First, the tweets prominently feature the WikiLeaks logo. *See* Special Agent Mander testimony, 10 June 2013 (describing WikiLeaks logo on the twitter page). Second, the tweets feature WikiLeaks' name as the account name "wikileaks" used on Twitter. *See id.* (stating that the handle of the Twitter account is "wikileaks") Similarly, the uniform resource locator (hereinafter "URL") for the WikiLeaks Twitter page is http://www.twitter.com/wikileaks. *See id.* Third, the content of the tweets relates to information compromised by the accused. *See id.* (discussing the content of the email tweet (PE 31 for Identification)). Content known by the author constitutes a proper basis for authentication. *See United States v. Siddiqui*, 235 F.3d 1318, 1322-23 (11th Cir. 2000) (determining emails were properly authenticated because, among other factors, they contained information known to the defendant); *see also Link v. Mercedes-Benz of N. Am., Inc.*, 788 F.2d

[1] A "tweet" is a message no longer than 140 characters posted on the website Twitter.com (hereinafter "Twitter"). Twitter New User FAQ, *available at* https://support.twitter.com/articles/13920-new-user-faqs# (last visited 15 June 2013). Twitter is an online social networking service that enables its users to send and read tweets. *Id.* By default, tweets are public, which allows anyone, with or without a Twitter account, to view all tweets from the public account. *See id.*

918, 927 (3d Cir.1986) (holding documents properly authenticated by direct testimony or the contents of the documents themselves) (emphasis added). Fourth, the Twitter page for WikiLeaks possesses over 1,800,000 followers. *See* Twitter Account labeled "WikiLeaks," *available at* https://twitter.com/wikileaks (last visited 15 June 2013). Here, Twitter users have overwhelmingly authenticated the WikiLeaks Twitter page. Fifth, the WikiLeaks web site linked to the twitter.com/wikileaks web site as recently as 4 June 2013. *See* Enclosure 1. Finally, the tweets still exist on twitter.com and are accessible to anyone on the Internet. *See* Special Agent Mander testimony, 10 June 2013 (stating the Twitter is available to the general public and that he reviewed the Twitter feed of the WikiLeaks account recently).

The email tweet (PE 31 for Identification) remains available on Twitter.com with the same date of 7 May 2010. *See id.* The video tweet (PE 32 for Identification) remains available on Twitter.com with the same date of 8 January 2010. *See id.* Outside sources referred to the WikiLeaks tweets in 2010. *See, e.g*, Enclosure 2. These sources are proper authority for considering the authenticity of the tweets. *See United States v. Bourjaily*, 483 U.S. 171, 175 (1987) (holding Federal Rule of Evidence 104 permits a Court to consider any evidence regarding admissibility); MRE 104 (stating that the military judge is not bound by the rules of evidence, except those with respect to privileges, in making determinations regarding the admissibility of evidence). The contents of the tweets and the tweets' distinctive characteristics authenticate the tweets as being from WikiLeaks. Furthermore, extrinsic evidence supports the proposition that the dates included on the tweets are accurate and therefore authentic. Thus, the email tweet (PE 31 for Identification) and video tweet (PE 32 for Identification) are authentic.

B. Internet Archive Results Are Authentic

1. Internet Archive Results Are Self-Authenticating with Affidavit

Self-authenticating evidence does not require "[e]xtrinsic evidence of authenticity as a condition precedent to admissibility." MRE 902. "Certified domestic records of regularly conducted activity" fall qualify as self-authenticating evidence. MRE 902(11). Pursuant to MRE 902(11), extrinsic evidence of authenticity as a condition precedent to admissibility is not required with respect to certified domestic records of a regularly conducted activity when:

> The original or a duplicate of a domestic record of regularly conducted activity that would be admissible under Mil. R. Evid. 803(6) if accompanied by a written declaration of its custodian or other qualified person, in a manner complying with any Act of Congress or rule prescribed by the Supreme Court pursuant to statutory authority, certifying that the record (A) was made at or near the time of the occurrence of the matters set forth by, or from information transmitted by, a person with knowledge of those matters; (B) was kept in the course of the regularly conducted activity; and (C) was made by the regularly conducted activity as a regular practice.

MRE 902(11). The sworn attestation states that the records accurately reflect the files as captured on the date detailed in the URL. *See* Enclosure 4. The attestation affirms that the "records were captured by the Internet Archive or received from third party donors in the course of regularly conducted activity by the Internet Archive." *See* Enclosure 4. The attestation affirms that capturing the records comprised "regularly conducted activity by the Internet Archive." *See* Enclosure 4. Because the records are stored, the act of capturing the record constitutes regularly making the record. *See* Enclosure 4. On 13 June 2013, the United States provided the Defense a copy of Enclosure 4 and notice of the United State's intent to file Enclosure 4. *See* Enclosure 5. Therefore, the attestation satisfies the requirements of regularly conducted business activities under MRE 803(6) and is self-authenticating under MRE 902(11).

2. Internet Archive Results Are Authentic in Accordance with Defense's Cited Precedent

MRE 901(b)(1) permits authentication based on personal knowledge. *See* MRE 901(b)(1). The sworn attestation states that the records accurately reflect the files as captured on the date detailed in the URL. *See* Enclosure 4. Moreover, the sworn attestation is based on personal knowledge of an automated process. *See id.* The Internet Archive URL is automatically assigned at the capture of the web site by the Internet Archive. *See id;* Enclosure 3. Where the electronic records are merely stored in a computer, there is no "computer-specific" authentication issue. *Lubich*, 72 M.J. at 174 (citing 5 Weinstein & Margaret A. Berger, *Weinstein's Federal Evidence* § 900.06[3], at 900-68 (Joseph M. McLaughlin ed., 2d ed. 2003)). The Internet Archive does not process web sites; it stores them. *See* Enclosure 3 (stating that the Internet Archive is a digital library). Special Agent Mander testified regarding the process by which he personally searched for the file. Because the United States has now presented a sworn attestation confirming the accuracy of Special Agent Mander's results and, along with the sworn testimony of the process by which the stored results were retrieved, any doubts about the process of storing the results on the Internet Archive relate to the weight of the evidence, not its admissibility. *See Lubich*, 72 M.J. at 175 (determining accuracy of printout affects weight, not admissibility, after *prima facie* showing of authenticity); *see also United States v. Johnson*, 68 F.3d 899, 903 (5th Cir. 1995) (noting that, after *prima facie* showing of authenticity, gaps in chain of evidence go to weight, not admissibility).

The authority presented by the Defense holds that an affidavit verifying the accuracy of the results from the Internet Archive by an Internet Archive representative with personal knowledge of its contents satisfies the requirement for authentication. *See St. Luke's Cataract and Laser Institute, P.A. v. Sanderson*, 2006 WL 1320242 (M.D. Fla. 2006); *Telewizja Polska USA, Inc. v. Echostar Satellite Corp.*, 2004 WL 2367740 (N.D. Ill. 2004); *see also United States v. Bansal*, 663 F.3d 634 (3d Cir. 2011) (holding testimony of a witness with personal knowledge sufficient to authenticate Internet Archive results). The records custodian attests that the records were duly maintained; the record custodian rarely has personal knowledge of their actual contents. *See United States v. Gladwin*, 34 C.M.R. 208, 214 (C.M.A. 1964) (noting that only in rare instances would a records custodian be able to assist the fact finder in determining the accuracy of stored records). Additionally, the *Telewizja* precedent cited by the Defense notes that the Internet Archive was a relatively new source for archiving websites in 2004. In 2013, the reliability of the Internet Archive has been established and tested. *Cf.* Deborah R. Eltgroth,

Best Evidence and the Wayback Machine: Toward a Workable Authentication Standard for Archived Internet Evidence, 78 Fordham. L. Rev. 181, 188-190 (2009) (describing history of courts relaxing the burden for authenticating photographs as the technology became more widespread). Recently, courts have relied on the results from the Internet Archive as accurate representations of the website as it existed on the date listed in the Internet Archive. *See, e.g.*, *Arteaga v. U.S.*, 711 F.3d 828 (7th Cir. 2013); *Santos ex rel. Beato v. U.S.* 559 F.3d 189 (3d Cir. 2009). Accordingly, the Internet Archive results are also authentic under MRE 901(b)(9). *See Lubich*, 72 M.J. at 175.

Moreover, the Internet Archive is an electronic library. A witness with direct knowledge of the process by which the library compiles the results is not required. *See Lubich*, 72 M.J. at 174-75 (rejecting defense arguments that direct testimony was required as to the process utilized to collect the data). Thus, after a *prima facie* showing of authenticity, any contrary evidence presented by the Defense goes to the weight of the Most Wanted List (PE 109 for Identification), not its authenticity. *See id.* at 175 (citing *United States v. Tank*, 200 F.3d 627, 630 (9th Cir. 2000)). The Defense may present contrary evidence, if any, during its case-in-chief to rebut any weight given to the Government's evidence. *See United States v. Thomas*, 33 M.J. 1067, 1068 (A.C.M.R. 1991) ("Of course, the appellant was free to dispute the authenticity of individual documents or present evidence that the person who signed the attesting certificate was not the custodian of the documents attached to it."), *rev'd on other grounds*, *United States v. Thomas*, 36 M.J. 378 (C.M.A. 1992).

However, in accordance with the precedent presented by the Defense, the United States encloses a notarized and sworn affidavit stating that the results from the Internet Archive are accurate depictions of the WikiLeaks website on 5 November 2009. *See* Enclosure 4. The affidavit explains that the Internet archive digitally stores websites on specific dates and makes the websites as they exist on the stated dates searchable to any Internet user. *See id.* The Internet Archive explains on its website the date format as:

> The Internet Archive assigns a URL on its site to the archived files in the format http://web.archive.org/web/[Year in yyyy][Month in mm][Day in dd][Time code in hh:mm:ss]/[Archived URL]. Thus, the Internet Archive URL http://web.archive.org/web/19970126045828/http://www.archive.org/ would be the URL for the record of the Internet Archive home page HTML file (http://www.archive.org/) archived on January 26, 1997 at 4:58 a.m. and 28 seconds (1997/01/26 at 04:58:28)

Internet Archive Standard Affidavit, *available at* http://archive.org/legal/affidavit.php (last visited 15 June 2013); Enclosure 3. Accordingly, the Most Wanted List's (PE 109 for Identification) relevant URL of "20091105061330" corresponds to a date of 5 November 2009 at 06:13:30.

Additionally, in chat logs admitted by the Court recovered from PFC Manning's personal computer, the accused and "pressassociation@jabber.ccc.de" discuss the "open source center." Through Mr. Mark Johnson, the United States presented evidence that

"pressassociation@jabber.ccc.de" was in fact Julian Assange, or at a minimum, that the accused believed that the user was Julian Assange. The same testimony noted that the accused originally assigned that username the alias "Nathaniel Frank." In the chat logs, "pressassociation@jabber.ccc.de" expresses interest in the mining of the open source center and the United States presented evidence that the 2009 Most Wanted List (PE 109 for Identification) sought the entire open source center. As such, the accused's conversation authenticates the Most Wanted List (PE 109 for Identification) by confirming the types of information desired by WikiLeaks and Julian Assange. Therefore, the United States has met its burden of demonstrating the authenticity of the Most Wanted List (PE 109 for Identification).

II. HEARSAY & RELEVANCE

A. Email Tweet (PE 31 for Identification) and Video Tweet (PE 32 for Identification)

The United States offers the email tweet (PE 31 for Identification) for the nonhearsay purpose of its effect on the accused. The tweet was published on Twitter on 7 May 2010. As charged, between on or about 11 May 2010 and on or about 27 May 2010, the accused stole the United States Forces-Iraq Microsoft Outlook/Sharepoint Exchange Server global address list (hereinafter "GAL"). *See* Charge Sheet. The accused regularly and thoroughly searched for information regarding WikiLeaks on sources such as Intelink. The accused admits to researching WikiLeaks in his online conversations with Mr. Lamo, saying, "[I]t took me four months to confirm that the person i [*sic*] was communicating [*sic*] was in fact assange [*sic*]." Given the large amount of research the accused conducted on WikiLeaks and the timing of the email tweet (PE 31 for Identification) and the accused's theft between on or about 11 May 2010 and on or about 27 May 2010, the fact finder can reasonably determine that the accused responded to the email tweet (PE 31 for Identification). The United States intends to elicit testimony by Special Agent Al Williamson, who conducted a forensic examination of a computer the accused was using from 11 May 2010 until 27 May 2010, that the accused stole the GAL between on or about 11 May 2010 and on or about 27 May 2010. The email tweet (PE 31 for Identification) is directly relevant to the accused's intent for compromising the GAL and potentially the value of the information. *See* Charge Sheet, Charge II Specification 16.

The email tweet (PE 31 for Identification) also demonstrates WikiLeaks plan to compromise military information as of 7 May 2010. *See* MRE 803(3). The plan, as openly and publicly advertised on Twitter, is relevant to the accused's knowledge of the scope of the disclosure of compromised information for Article 104. *See United States v. Roberson*, 65 M.J. 43, 46 (C.A.A.F. 2007) (concluding that statements showing declarant's willingness to get his money by any means necessary reflected his intent and were admissible to show both his intent and that the intent was subsequently carried out).

Furthermore, the video tweet (PE 32 for Identification) demonstrates WikiLeaks plan to compromise military information as of 8 January 2010. *See* MRE 803(3). The tweet also establishes the then-existing state of mind of the WikiLeaks declarant with respect to the nature of the possession. *See United States v. Elliott*, 23 M.J. 1, 8 (C.M.A. 1986) (holding declarant's statements regarding stolen property admissible to prove state of mind regarding possession). The plan and state of mind, as openly and publicly advertised on Twitter, are relevant to the

accused's knowledge of the scope of the disclosure of compromised information for Article 104. WikiLeak's plan to compromise the video is relevant to proving the charged act of compromising the Gharani video. *See Roberson, supra.*

Finally, the video tweet (PE 32 for Identification) is not offered for its literal truth, but rather what WikiLeaks' state of mind regarding the content of the videos. The tweet expresses WikiLeaks' belief about the content of the video. The video was encrypted, and thus WikiLeaks could not know the content of the encrypted video. The United States presented evidence through Special Agent David Shaver that at least one of the videos referred to by WikiLeaks in the tweet was in the possession of an individual named Jason Katz. This video, present on Mr. Katz's computer on 15 December 2009 and matching a video on the CENTCOM SharePoint server in the "Farah" investigation folder, was flyover footage and not video of a bomb strike at all. Both the video on Mr. Katz's computer and the videos in the Farah investigation folder on the United States Central Command SharePoint server were password protected, meaning that individuals without the password could not examine the contents of the video. Thus, the tweet is not being offered for its truth, but rather what WikiLeaks was told about the content of the videos. The accused, in chat logs with Mr. Lamo, confirmed that the Farah or Gharani videos were "encrypted," that the password had not been broken yet, and that he understood the videos to depict bomb strikes on civilians. The admission to Mr. Lamo further corroborates the characterization given to WikiLeaks by the accused.

B. Most Wanted List (PE 109 for Identification)

MRE 803(6) excepts the Most Wanted List (PE 109 for Identification) from the rule against hearsay. The attestation affirms that the "records were captured by the Internet Archive or received from third party donors in the course of regularly conducted activity by the Internet Archive." *See* Enclosure 4. The attestation affirms that capturing the records comprised "regularly conducted activity by the Internet Archive." *See* Enclosure 4. Because the records are stored, the act of capturing the record constitutes regularly making the record. *See* Enclosure 4. Thus, the Most Wanted List (PE 109 for Identification) meets a hearsay exception in conjunction with the sworn and notarized affidavit in Enclosure 4. *See* MRE 803(6).

The United States also offers the Most Wanted List (PE 109 for Identification) for the nonhearsay purpose of its effect on the accused. The use of the Most Wanted List (PE 109 for Identification) by the accused is relevant to his course of conduct in the late November 2009 timeframe and his knowledge of WikiLeaks. The accused admitted, "I gathered more info when I questioned him . . . ." PE 120. The accused admits to helping WikiLeaks after Thanksgiving of 2009. *See* Special Agent David Shaver testimony, 11 June 2013 (stating Intelink searches began in November 2009); PE 30 (stating accused's admission that he began helping WikiLeaks after release of 9/11 pager data). The accused also created a text file containing contact information for Julian Assange on 29 November 2009. *See* Mr. Mark Johnson testimony, 12 June 2013. The accused began searching on Intelink for terms or information appearing on the Most Wanted List (PE 109 for Identification) in late November 2009 and into early December 2009. *See* Special Agent Shaver testimony, *supra.* This conduct related to WikiLeaks in late November tends to corroborate the accused's admissions that he began helping WikiLeaks in

November 2009 and that he transmitted the video charged in Specification 11 of Charge II around that same time.

Finally, the accused specifically discussed monitoring the CIA Open Source center with Mr. Assange, who expressed interest in having the entire Open Source center "mined." *See* Mr. Mark Johnson testimony, *supra.* Therefore, the Most Wanted List (PE 109 for Identification) is evidence of the accused's intent with regard to all data he compromised. The Most Wanted List (PE 109 for Identification) demonstrates desire of WikiLeaks to publish the information and is admissible as WikiLeaks' then-existing plan under MRE 803(3). *See Roberson, supra.* The United States intends to prove that the accused adopted the plan as he admitted both to Mr. Assange and Mr. Lamo. In communicating with Mr. Lamo, the accused refers to himself as a "source." *See* PE 30. Thus, the Most Wanted List (PE 109 for Identification) is also relevant because it makes it more likely WikiLeaks would publish information received that was requested in both the Most Wanted List (PE 109 for Identification) and other information discussed with Mr. Assange.

CONCLUSION

The email tweet (PE 31 for Identification) and video tweet (PE 32 for Identification) are authentic based on their distinctive internal characteristics and the accused's acts. The Most Wanted List (PE 109 for identification) is authentic as an accurately recorded record. The email tweet, video tweet, and Most Wanted List (PE 109 for Identification) explain the course of the accused's charged acts. The explanation of the accused's acts constitutes evidence of the accused's intent, plan, and knowledge and is therefore relevant.

ALEXANDER S. VON ELTEN
CPT, JA
Assistant Trial Counsel

Enclosures
1. Internet Archive Capture of WikiLeaks Link to WikiLeaks' Twitter Account
2. 7 May 2010 Article Referencing WikiLeaks' Email Tweet
3. Internet Archive Sample Affidavit
4. Internet Archive Attestation
5. MAJ Fein Email, 13 June 2013

I certify that I served or caused to be served a true copy of the above on Mr. David Coombs, Civilian Defense Counsel via electronic mail, on 15 June 2013.

ALEXANDER S. VON ELTEN
CPT, JA
Assistant Trial Counsel